Available online at www.sciencedirect.com

ScienceDirect

Procedia - Social and Behavioral Sciences 90 (2013) 923 – 930

Procedia
Social and Behavioral Sciences

6th International Conference on University Learning and Teaching (InCULT 2012)

Student perception on security requirement of e-learning services

Zainal Fikri Zamzuri[a], Mazani Manaf[b], Yuzaimi Yunus[c], Adnan Ahmad[d]

[abcd] *Faculty of Computer and Mathematical Science,*
Universiti Teknologi MARA, Shah Alam, Selangor, 40450, Malaysia

Abstract

All the web based systems are exposed to computer security threats. This is one of the main reasons why people are reluctant to use the web based system including the e-learning system. It is very important to understand the needs and fears of users when they use the e-learning system. This paper analyzed user perception on the e-learning security system. Questionnaires were distributed to the students to get their responses on the e-learning security system. The feedback from the students was analyzed using statistical software. STRIDE threat modeling was used to identify the critical area in the e-learning system. The results show that students are concerned with the integrity and availability of the system. They do not mind if other people know what their activities are in the system. The most critical service compared to other services offered by the e-learning system is the assessment service.

Keywords: e-learning system; STRIDE; e-learning services;e-learning security; computer security threats ;

1. Introduction

E-learning system is a compulsory tool in the education system nowadays. The usage of the E-learning system can increase the productivity of the institution since it can be accessed by users 24 hours. Most of the e-learning systems provide services such as forums, emails, online assessments, learning resources and notices which allow the users to communicate irrespective of time and space. Since it is a web based system, it is exposed to computer security threats. In the globalized era where collection and storage of user information happens even without

* Corresponding author.
E-mail address: zfikri2008@yahoo.com

doi:10.1016/j.sbspro.2013.07.169

permission of the users (students, patients, pilots, passengers etc.), addressing privacy and security issues are therefore vital and all necessary steps need to be taken to ensure that information is properly secured, especially within the e-learning system (Bevanda, Azemovic, & Mušic, 2009).

Students are the biggest users of the e-learning system. Students are concerned about their privacy and security when using the e-learning system. They worry that confidential information such as their assessment marks and what they are doing might be revealed to others. They also need a reliable system to avoid being frustrated when using the system which can influence their study performance. Needs and views of students as the biggest users of the e-learning system are important to be considered to ensure that the system is successfully implemented in any institution. One of the reasons why people reject the online system is due to computer security reasons. Availability, integrity and confidentiality are the computer security components.

The online users using the system are worried they will lose their privacy, the confidentiality of their sensitive information and the availability of the system when they need it. In the e-learning system, users would feel more confident in interacting and collaborating with others when there are mechanisms in place to create the privacy, trust and a secure environment. Student perception of the service quality of an e-learning system is important since the students can offer insights into the conditions that reduce service quality in e-learning, and they experience the institution's service delivery system day after day (Hilmi, Pawanchik, & Mustapha, 2011). Graf (2002); El-Khaib, Korba et al. (2003); Davis (2004) and Saxena (2004) agreed that the role of security in e-learning system is to provide a secure end-to-end session between the student and the institution's e-learning network (Raitman, Ngo, Augar, & Zhou, 2005). The objectives of this paper are to identify which security components are high risks to the e-learning system and which e-learning system services are high risks to the e-learning system. The findings of this paper can help the e-learning system developer to put more security on the components and services of the e-learning system that are exposed to the computer security threats. Gehling & Stankard (2005) stressed that it is very important to know and understand all the threats towards the system that is to be developed in the assessment phase.

2. Related researches

There are a few studies which have been done on student and user perception towards the e-learning system. Buzzetto-More & Koohang (2009) did a research on student perception of various e-learning components. They found that the e-learning system can enhance students' understanding of the course content they study and this will give an impact on higher education. Selim (2007) revealed that students perceived instructor characteristic as the most critical factor in the success of e-learning. Mohd Alwi (2009) who studied the perception of e-learning practitioners found that their respondents agreed that there are security threats in e-learning and good security management in e-learning is important in securing the e-learning environment.

3. E-learnıng servıces

Zamzuri, Manaf, Ahmad, & Yunus (2011) defined e-learning asset as services provided by the e-learning system such as learning resources, examination or assessment questions, students' results, user profile, forum contents, students' assignments and announcements in the e-learning system.

Learning resources are assets that provide students with lecture notes to help students in their studies. Learning resources are uploaded by the facilitators for their students. Students hope that the learning resources such as the lecture notes that they download from the system have not been changed from the original content.

Examinations or on-line assessments are an asset thus the privacy, integrity and availability of these assets have to be guarded carefully. The exam questions and students' answer sheets have to be protected from being tampered to ensure the integrity of the examination. Students should not know the questions before an exam is conducted to ensure the confidentiality of the examination.

Mark service is keeping information about a student's performance such as continuous assessments, assignments and examination results. This information should be known by the owner only. This asset can only be accessed by the student and the facilitator. The facilitator will key in and update the information of this asset.

Profiles of students, facilitators and administrators will be keyed-in by the administrator using the profile service. The student and facilitator can only update certain profiles themselves once their records already exist in the system.

The forum service is used by students and facilitators for discussions. Students can send questions and wait for responses from other students or facilitators. Some of the discussions probably involve a sensitive issue; therefore the privacy of this forum must be protected.

Announcement service is used by the administrator and facilitator to disseminate information to the users especially to students.

The assignment service allows students to download assignment questions and submit their assignments. Students submit their assignments by uploading their work into the system. Most students use this e-learning system to download lecture notes, reading materials, announcement, and feedback from the forum, submitting assignments and questions to the forum, checking assessment marks and sitting for an examination or assessment. They expect all information in the system to be error-free, is available when they want to use it, and it is confidentiality protected.

4. STRIDE

A threat is an adversary's goal, or what an adversary might try to do to a system. In general, threats can be classified into six classes based on their effect (Swiderski & Snyder, 2004). The six categories of computer threats are in line with STRIDE threat modelling. STRIDE is a method used to classify the identified threats. STRIDE is a classification scheme for characterizing known threats according to the kinds of exploit that are used (or motivation of the attacker). The STRIDE (Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) acronym is formed from the first letter of each of the following categories as shown in Figure 1.

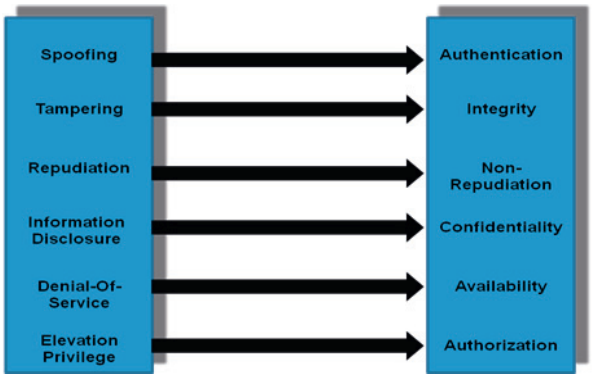

Figure1. *E-learning security conceptual framework*

Authorization will give an impact on integrity, confidentiality and availability.

5. Methodology

About 200 questionnaires were distributed to the students. One hundred and fourteen were chosen to be analysed after validating the questionnaires. Questionnaires were used to get feedback from students using the e-learning system. The questionnaire was divided into three sections where section B was the main section with six sub-sections. The first until the third sub-section in section B were questions about computer security in the e-learning system. The fourth sub-section looked at student awareness of computer security whereas the fifth sub-section was about students' computer competency level. The last sub-section was about the benefit of e-learning system to students. Most of the questions were structured using the five point likert scale ranging from 1=strongly disagree to 5=strongly agree. Statistical software was used to analyse the data. In this paper, the mean value was used to calculate the risk level for each factor and service.

The STRIDE method was used to identify the critical areas in the e-learning system based on the response from the questionnaires. Writers only concentrated on the tampering, information disclosure and denial-of-service categories in the STRIDE methodology. These categories are associated with the use of e-learning system by students. In order to rate the critical level for each factor, the mean value of the question was used. If more than one question were asked, the average mean value was used.

To calculate the critical value for each service, the average of the critical level was used as shown below.

Rf = the risk level for each factor in STRIDE

Rf = Average of mean for the factor in STRIDE number of questions

$$Rf(Xi) = \sum_{j=1}^{n} uj \quad (1)$$

μ = the mean value for each factor
n = number of questions

To calculate the risk for each service
Rs = risk value for each service
Rs = the risk value for each factor (Rf) in the service number of factors

$$Rs\ (service) = \frac{\sum_{i=1}^{m} Rf(Xi)}{m} \quad (2)$$

Where m is a number of factor in STRIDE and = 1, 2 or 3.

6. Analysis and finding

6.1. Learning resources

Tampering

About 93% of the respondents did not feel happy if the learning resources they downloaded from the system were not accurate. They believed that all the learning resources and contents in the system are error free. The mean value for this criterion is 3.32

Information disclosure

Approximately 24% of the respondents did not like people to know that they downloaded the learning resources from the system. Most of the respondents did not mind if other people knew that they downloaded the learning resources from the system. The mean value for this criterion is 1.92

Denial of Service

The learning resources must be available when they need them. About 85% of the respondents could not accept that the learning resources are not available either because the e-learning system is not available or the learning resources are not available (removed from system). The mean value for this criterion is 3.28

6.2. Forum services

Tampering

About 98% of the students did not feel happy if the question they sent to their lecturer had been modified without their knowledge. The mean value for this criterion is 3.5

Information disclosure

The students did not mind if other people knew that they sent questions and took part in forum discussions. About 41% of the respondents did not seem happy if people knew they were discussing sensitive questions. The mean value for this criterion is 1.81.

Denial of Service

Most students needed the forum services to exchange ideas and discuss with their friends and lecturers. About 88% of the respondents really used the forum service to discuss and ask questions. They also needed this service to send questions to their lecturers. The mean value for this criterion is 3.08.

6.3. User profile

Tampering

Students believed that the information about their lecturers and themselves are important. More than 96% of the respondents needed their profiles to be correct and 89% of the respondents wanted their lecturers' profiles to be accurate. The mean value for this criteria is 3.35.

Information disclosure

About 78% of the respondents did not like it if their profiles had been distributed without their knowledge. The mean value for this criterion is 3.04.

Denial of Service

The students were interested to know their lecturers' profiles and about 89% of the respondents wanted the system to always be available for them to update their profiles. The mean value for this criterion is 3.01.

6.4. On-line assessment service

Tampering

About 98% of the respondents were not happy if there was a change made to their assessment answers without their knowledge. The students were also not happy if they received the wrong assignment questions. The mean value for this criterion is 3.47.

Information disclosure

The students felt cheated if their course mates knew of the assessment questions before the assessment was held. The mean value for this criterion is 3.86.

Denial of Service

77% of the students were not happy if an assessment was delayed when they were ready for the assessment. The mean value for this criterion is 2.95.

6.5. E-mail service

Tampering

About 96% of the respondents did not like any changes to be made to their email content without their knowledge. The mean value for this criterion is 3.54.

Information disclosure

The students did not like their email to be read but they did not mind if other people knew that they have sent and received emails from the lecturers. The mean value for this criterion is 2.46.

Denial of Service

Most of the students i.e. 90% of the respondents needed the email service to communicate with lecturers and course mates. The mean value for this criterion is 3.18.

6.6. Mark service

Tampering

Any changes made to the students' assessment and assignment marks without their knowledge would make the students unhappy. The mean value for this criterion is 3.47.

Information disclosure

Only about 13% of the respondents did not mind if other people knew their assessment marks. The students did not feel happy if other people know their marks. They felt that their study performance was private. The mean value for this criterion is 2.88.

Denial of Service

86% of the respondents felt that it was necessary for them to be able to know their assessments marks when they need it. The mean value for this criterion is 3.86.

6.7. Announcement service

Tampering

Most of the students hoped that the information in the announcement service was correct. About 94% of the respondents could not accept if the information in the announcement service is not accurate. The mean value for this criterion is 3.37.

Denial of Service

The students depended on this service to get up-to-date information. About 88% of the respondents needed this system to be available when they need it. The mean value for this criterion is 3.2.

6.8. Critical Level of Security Components and E-Learning Services

Table 1 below shows the critical level for each service according to the security components. The critical level of the security components in the e-learning system is shown in Table 2.

The results show that the assessment service is the most critical service in the e-learning system. The students believed that if the assessment service is not protected well it would jeopardize their study performance.

The privacy, integrity and availability of these assets have to be guarded carefully. The examination questions and students' answer sheets have to be protected from being tampered with to ensure the validity and reliability of the examination.

Table 1. Critical level of the e-learning services

No.	Services	Denial of service	Tampering	Information disclosure	Average
1	Assessment	2.95	3.47	3.86	3.43
2	Marks	3.86	3.47	2.88	3.40
3	Profile	3.01	3.35	3.04	3.13
4	E-Mail	3.18	3.54	2.46	3.06
5	Learning Resources	3.28	3.32	1.92	2.84
6	Forum	3.08	3.5	1.81	2.80
7	Announcement	3.32	3.37	-	3.35

Table 2. Critical level of e-learning security components

No.	Security Components	Assessment	Marks	Profile	E-Mail	Learning Resources	Forum	Announcement	Average
1	Tampering	3.47	3.47	3.35	3.54	3.32	3.5	3.37	3.43
2	Denial of service	2.95	3.86	3.01	3.18	3.28	3.08	3.32	3.24
3	Information disclosure	3.86	2.88	3.04	2.46	1.92	1.81	-	2.66

Zamzuri, et al. (2011) also classify on-line assessment service as restricted or at level three for critical level since it will give a significant impact on the institution when the data is unauthorized for disclosure and alteration by unauthorized people and disruptions of access. Marais, Argles, and Von Solms (2006) suggested a method which allows a test to be retrievable once. This method protects the integrity of that assessment.

The students chose the announcement service as the most needed service to be available when they need. It shows that the students are dependent on the announcement for up-to-date information such as information about their class, assessment schedule, faculties and university activities, etc. They also need the information in the announcement to be error free.

The assessment and mark services have higher risk compared to other services for the information disclosure criteria. A student has the right to keep his/her marks and information private and confidential (Marais, et al., 2006). Students also want their user profiles not to be distributed without their permission. This is in line with May, Fessakis, Dimitracopoulou and George (2012) who found in their research that e-learning users urgently needed protection of their personal data.

All the services recorded high risk for integrity security component. It shows that students cannot accept information which is not accurate. Tutănescu and Sofron (2003) assert that data modification and disinformation attacks are threats to the integrity security component which gives more bad impact to the system compared to other attacks.

For the security components, the students chose integrity as the critical security component in the e-learning system. The results show that students were so concerned about the tampering of data that can adversely affect their learning performance. Integrity attack is classified as an active attack which represents an attack that modifies (through insertion and/or deletion of characters) a part or all transmitted data (Tutănescu & Sofron, 2003). A consequence of integrity attack is that the authorized users i.e. students, can have access to the e-learning system but what they find in the system is not as expected. Bertino, Bruschi, Franzoni, Nai-Fovino, and Valtolina (2005) suggested that SQL-Injection and unauthorized access attacks are the two common threats to integrity.

7. Conclusions

As the main users, students' feedback is important to ensure that the e-learning system is successfully implemented in the institution. The system developer and administrator need to make sure that the information in the system is error-free since that will ensure that students will have confidence to use the system. The system developer also has to pay more attention on the components and services which are exposed to security threats to make the users more confident to use the e-learning system. Further research on how e-learning system developers respond to the needs of students' is required.

Acknowledgements

This study acknowledges the support of the Malaysian Ministry of Higher Education for the Fundamental Research Grant Scheme (FRGS) under contract number 600-RMI/ST/FRGS5/3/FST (237/2010).

References

Bertino, E., Bruschi, D., Franzoni, S., Nai-Fovino, I., & Valtolina, S. (2005). *Threat modelling for SQL Servers*.

Bevanda, V., Azemovic, J., & Mušic, D. (2009). *Privacy preserving in eLearning environment (Case of modeling Hippocratic database structure)*.

Buzzetto-More, N. A., & Koohang, A. (2009). Student perceptions of various e-learning components. *International Journal of Doctoral Studies, 4*, 113-135.

Gehling, B., & Stankard, D. (2005). *eCommerce security.* Paper presented at the Proceedings of the 2nd annual conference on Information security curriculum development.

Hilmi, M. F., Pawanchik, S., & Mustapha, Y. (2011). *Exploring security perception of learning management system (LMS) portal*.

Marais, E., Argles, D., & Von Solms, B. (2006). Security issues specific to e-assessments. *The International Journal for Infonomics*.

May, M., Fessakis, G., Dimitracopoulou, A., & George, S. (2012). *A Study on User's Perception in E-learning Security and Privacy Issues*.

Mohd Alwi, N. a. I.-S., F. (2009). *User's Perception in Information Security Threats in E-Learning.* Paper presented at the 2nd International Conference of Education, Research and Innovation, Madrid, Spain.

Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). *Security in the online e-learning environment*.

Selim, H. M. (2007). E-learning critical success factors: an exploratory investigation of student perceptions. *International Journal of Technology Marketing, 2*(2), 157-182.

Swiderski, F., & Snyder, W. (2004). *Threat modeling* (Vol. 14): Microsoft Press.

Tutănescu, I., & Sofron, E. (2003). *Anatomy and types of attacks against computer networks*.

Zamzuri, Z. F., Manaf, M., Ahmad, A., & Yunus, Y. (2011). Computer Security Threats Towards the E-Learning System Assets. *Software Engineering and Computer Systems*, 335-345.